DEMISTO
A PALO ALTO NETWORKS® COMPANY

INTEZER

Automated Malware Analysis and Response

Benefits

- Execute Intezer's Genetic Malware Analysis within Demisto in real time.
- Accurately identify threats, classify them according to risk and severity, and provide deep insights into every single alert.
- Shorten analysis, decision-making, and response cycles by automating key tasks with analyst review.

Compatibility

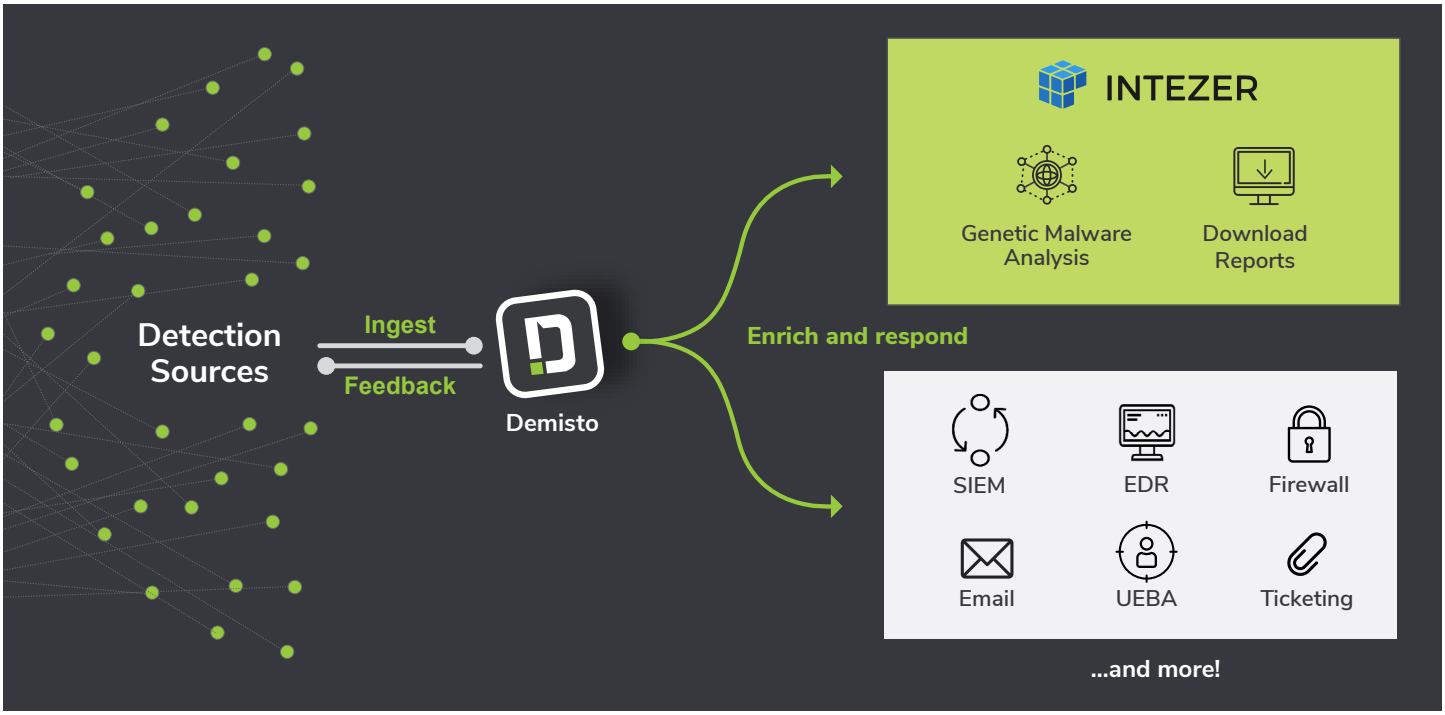
- Products: Demisto Enterprise, Intezer Analyze
- Platform: Platform independent

For many organizations, thousands of alerts are generated by security systems every day, making it impossible for security teams to prioritize files according to risk and severity without having to weed through false positives. As a result, valuable time is wasted between detection and response, while threats continue to manifest within the network. Shortening the investigation process and response time is a constant security challenge. Analysts need a solution that helps them focus on what's critical and reduces their mean time to respond.

The **Intezer** and **Demisto** integration equips security teams with an efficient workflow for **security orchestration, malware analysis**, and **incident response**. Organizations are empowered to improve malware analysis accuracy with code reuse and similarity detection for every single alert. They also get relevant context into any suspicious files to help them accelerate response time.
In addition, Demisto provides a unified platform to coordinate malware analysis with other security processes, giving analysts rich incident context, automated actions, and a collaborative workspace to accelerate incident response.

Integration features:

- Orchestrate Intezer's Genetic Malware Analysis into an existing security pipeline through task-based playbooks.
- Automatically analyze any suspicious file with Intezer Analyze within Demisto to obtain a comprehensive report, including the verdict and malware family classification.
- Trigger automated playbooks within Demisto to add accurate context to alerts.
- Leverage hundreds of Demisto product integrations to further enrich Intezer data and coordinate responses across security functions.
- Run thousands of commands (including for Intezer) interactively via a ChatOps interface while collaborating with other analysts and Demisto's chatbot.



USE CASE #1 AUTOMATED MALWARE ANALYSIS AND VALIDATION

Challenge: SOC and incident response teams spend resources in the form of time and analysis efforts on false positives. They must be able to prioritize alerts according to risk and severity without missing critical incidents.

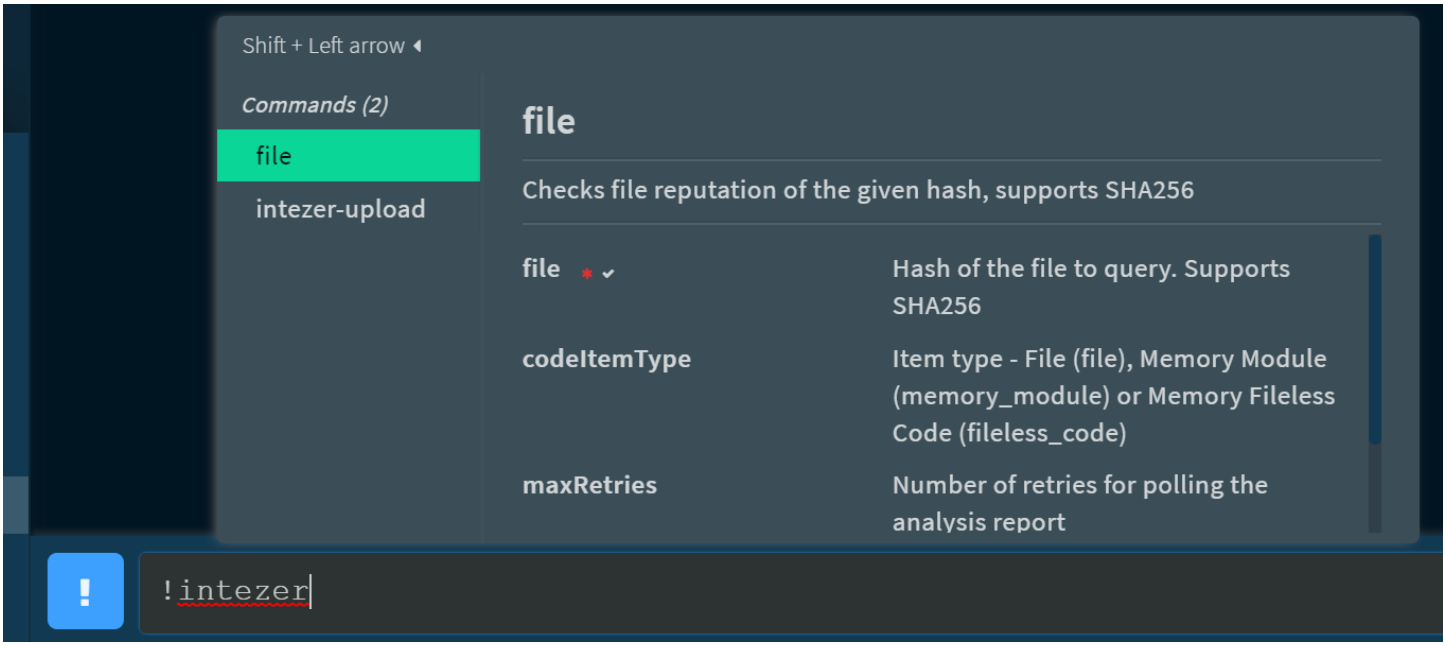
Solution: SOCs can have standardized playbooks that run automatically and query Intezer for malware analysis. Invoking a pre-designed Demisto playbook will automatically upload any suspected file or hash to Intezer Analyze. Intezer's Genetic Malware Analysis will analyze and classify the file or hash based on code reuse and similarities. The file will be deeply analyzed at the machine-code level and classified as legitimate or malicious to give SOC teams the insights needed for incident evaluation. If an incident poses a higher risk, security teams can respond quickly and effectively to ensure the threat does not spread through the network.

Benefit: SOC teams deploying this integration will achieve accurate malware analysis at scale, enabling them to instantly investigate and classify malware alerts within seconds. False positives will be reduced with the identification of code reuse in trusted and malicious software. The solution will help analysts prioritize alerts based on verdict, classification, and the threat actor behind the attack, shortening the time from detection to response from hours to minutes. Also, by aligning malware analysis with other concurrent security functions, these playbooks ensure that security teams have central visibility over incident response processes.

USE CASE #2 MALWARE INCIDENT CLASSIFICATION AND ENRICHMENT

Challenge: Beyond the standard incident response process, attack investigations also require accurate context-based analysis of threats and relevant actionable intelligence to better target response. However, this process is typically done manually and requires a high level of understanding and expertise. Unfortunately, there is a skills gap where many organizations do not have a dedicated team of malware experts adept at reverse engineering.

Solution: After running an automated malware analysis playbook, analysts can gain greater visibility and obtain new actionable information about the attack by running Intezer commands interactively in the Demisto War Room. For example, after detecting the file as malicious, analysts will receive additional enriched information.
Whether the threat is a nation-sponsored attack or a generic piece of malware, security teams are armed with critical insights such as string reuse, malware family, related samples, and threat actor attribution, enabling them to better understand what threat they are facing and tailor the right response accordingly.



Benefit: Threats are automatically classified according to the relevant malware family and threat actor, providing context which is crucial for security teams in remediation. This helps the incident response team make better decisions by understanding the capabilities or intent of malware. By providing insights on automated reverse engineering, Demisto and Intezer can help bridge technical skill gaps within SOC teams.

Additionally, the War Room enables all participating analysts to have full task-level visibility of the process followed, run and document commands from the same window, and prevent the need for collating information from multiple sources for documentation.

About Demisto
Demisto is the only Security Orchestration, Automation, and Response (SOAR) platform that combines security orchestration, incident management, and interactive investigation to serve security teams across the incident lifecycle. Our orchestration engine coordinates and automates tasks across 100s of partner products, resulting in an increased return on existing security investments. Demisto enables security teams to reduce Mean Time to Response (MTTR), create consistent incident management processes, and increase analyst productivity. For more information, visit www.demisto.com or follow @demistoinc on Twitter.

About Intezer
Intezer is replicating the concepts of the biological immune system into cyber security, offering enterprises unparalleled threat detection and accelerated incident response. By providing a fast, in-depth understanding of any file by mapping its code DNA at the 'gene' level, offering the most advanced level of malware detection and analysis. Intezer is able to detect code reuse from known malware, as well as code that was seen in trusted applications. Intezer was founded by experienced cyber security professionals including the founder of CyberArk, and the former head of IDF CERT. For more information, visit www.intezer.com or @Intezerlabs on Twitter.